UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/728,800	12/01/2000	Niels Mache	450117-02961	5593

20999 7590 04/23/2004

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	6

DATE MAILED: 04/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/728,800	MACHE, NIELS	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 December 0200*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on December 01, 2000. Claims 1-19 were received for consideration. A preliminary amendment for the claims were received and taken into consideration in the examination of the claims. Claims 1-19 are currently being considered.

Information Disclosure Statement

2. An initialed and dated copy of Applicant's IDS form 1449, Paper No. 2, is attached to the Office action.

Specification

3. The disclosure is objected to because of the following informalities: The first sentence on Page 3 of the Specification needs to be rewritten "According to the present invention, a method for the authentication of data communicated from an originator to a destination is provided."

The word "key" is missing after the statement "of second random data and the private," on page 5, line 6.

Appropriate correction is required.

Claim Objections

4. Claim 10 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 10 refers to a "Software program" which implements the method of claim 5. This does not further limit the claim, but in fact broadens the claim.

5. Claims 1 and 11 are objected to because of the following informalities: "characterized in that" has a different font and/or spacing than the rest of the claims section. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 10 recites the limitation "Software program" in the first line of the claim. There is insufficient antecedent basis for this limitation in the claim 5 in which claim 10 depends.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Misra et al. (U.S. Patent 5,757,920).

Regarding claim 1, Misra discloses:

Method for the authentication of data communicated from a originator to a destination, wherein a keyed hashing technique is used, according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function, and the data are transmitted together with the digest of the hash function from the originator to the destination,

characterized in that

the data comprises temporal validity information representing the temporal validity of the data (Figure 2A, column 5 line 47 – column 6 line 31).

Regarding claim 5, Misra discloses:

Method for the authenticated transmission of messages, comprising the following communication setup steps:

generating a login key by a keyed-hashing method on the basis of random data, temporal validity information and a private key (column 5 line 47 – column 6 line 31);

transmitting the login key from an originator to a destination (column 7 lines 10-21); and

verifying the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest on the destination side (column 8 lines 45 – 65).

Regarding claim 11, Misra discloses:

Distributed system for communicating authenticated data from a originator to a destination, designed for a keyed hashing technique according to which data to be authenticated is concatenated with a private key and then processed with a cryptographic hash function, and the data are transmitted together with the digest of the hash function from the originator to the destination,

characterized in that

the data comprises temporal validity information representing the temporal validity of the data (Figure 2A, column 5 line 47 – column 6 line 31).

Regarding claim 15, Misra discloses:

Distributes system for the authenticated transmission of messages, comprising:

an originator designed to generate a login key by a keyed-hashing method on the basis

of random data, temporal validity information and a private key (column 5 line 47 – column 6 line 31);

a network for transmitting the login key from the originator to a destination (column 7 lines 10-21),

wherein the destination is designed to verify the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest (column 8 lines 45 – 65).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Misra discloses:

Method according to claim 1, characterized in that the temporal validity information can be defined by the originator (column 5 line 47-55).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Misra discloses:

Method according to anyone of the preceding claims, characterized in that the data comprises random data which are unique for a time span defined by the temporal validity information (column 5 line 47-55).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Misra discloses:

Method according to anyone of the preceding claims, characterized in that the data is a login key for a communication setup and/or a message (column 5 lines 47-55).

Misra describes a session key (Figure 2A item 120), which is analogous to the login key delineated in above claim 4.

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Misra discloses:

Method according to claim 5,

furthermore comprising the following acknowledgement steps:

in case the verification of the authenticity and the temporal validity of the login key is positive, generating an acknowledgment key by a keyed-hashing method on the basis of second random data and the private key (column 8 lines 45 – 65);

transmitting the acknowledgment key from the destination to the originator (Figure 4B, column 8 lines 60-65); and

verifying the acknowledgment key by the originator (column 8 line 66 – column 9 line 9).

Claim 8 is rejected as applied above in rejecting claim 6. Furthermore, Misra discloses:

Method according to claim 6 or 7, furthermore comprising the following message transmission steps: in case the verification of the acknowledgment key is positive, extracting the second random data from the acknowledgment key, generating a message by a keyed-hashing method on the basis of the second random data, message data and the private key, transmitting the message from the originator to the destination, and, verifying the message by the destination (column 8 line 66 – column 9 line 9).

Claim 10 is rejected as applied above in rejecting claim 5. Furthermore, Misra discloses:

Software program product, characterized in that it implements, when loaded into a computing device of a distributed system, a method according to claim 5 (column 5 line 47 – column 6 line 31, column 7 lines 10-21, column 8 lines 45 – 65).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Misra discloses:

Distributed system according to claim 11, characterized in that the originator is designed to define the temporal validity information (column 5 line 47-55).

Claim 13 is rejected as applied above in rejecting claim 11. Furthermore, Misra discloses:

Distributed system according to claim 11, characterized in that the data comprises random data which are unique for a time span defined by the temporal validity information (column 5 line 47-55).

Claim 14 is rejected as applied above in rejecting claim 11. Furthermore, Misra discloses:

Distributed system according to claim 11, characterized in that the data is a login key for a communication setup and/or a message (column 5 lines 47-55).

Misra describes a session key (Figure 2A item 120), which is analogous to the login key delineated in above claim 4.

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Misra discloses:

Distributed system according to claim 15 wherein the destination is designed to generate an acknowledgment key by a keyed-hashing method on the basis of second random data and the private key and to transmit the acknowledgment key to the originator in case the verification of the authenticity and the temporal validity of the login key is positive (Figure 4B, column 8 lines 60-65); and
the originator is designed to verify the acknowledgment key (column 8 line 66 – column 9 line 9).

Claim 18 is rejected as applied above in rejecting claim 16. Furthermore, Misra discloses:

Distributed system according to claim 16 or 17, characterized in that the originator is designed to extract the second random data from the acknowledgment key in case the verification of the acknowledgment key is positive, generate a message by a keyed-hashing method on the basis of the second random data, message data and the private key, and transmit the message to the destination, and the destination is designed to verify the message (column 8 line 66 – column 9 line 9).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Misra discloses:

Method according to claim 8, characterized in that the message furthermore comprises a time stamp and when verifying the message it is checked on the basis of the time stamp and the temporal validity information whether the message is still valid (column 5 line 47 – column 6 line 31).

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Misra discloses:

Distributed system according to claim 18, characterized in that the message furthermore comprises a time stamp and when verifying the message, the destination checks on the basis of the time stamp and the temporal validity information whether the message is still valid (column 5 line 47 – column 6 line 31).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 7-8, and rejected under 35 U.S.C. 103(a) as being unpatentable over Misra et al. (U.S. Patent 5,757,920).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Misra discloses:

The acknowledgement key being verified at the originator. Misra does not explicitly disclose the acknowledgement key comprising a time stamp and a temporal validity information. However, by the basis of Misra invention, the original messages had a time stamp and temporal validity information that the time stamp is compared, to insure that the original session key has not expired. The functionality that exists in providing the first session key can easily be applied to the second session key which is provided by the destination. The time stamping and temporal validity information being added to the session key would provide a second layer of assurance that the key is valid, in addition to the second session key being encrypted with a private key of the destination.

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Misra discloses:

Distributed system according to claim 16, characterized in that there is an acknowledgement key which is verified at the originator. Misra does not explicitly disclose the acknowledgement key comprising a time stamp and a temporal validity information. However, by the basis of Misra invention, the original messages had a time stamp and temporal validity information that the time stamp is compared, to insure that the original session key has not expired. The functionality that exists in providing the first session key can easily be applied to the second session key which is provided by the destination. The time stamping and temporal validity information being added to the

session key would provide a second layer of assurance that the key is valid, in addition to the second session key being encrypted with a private key of the destination.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 703-305-8892. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-3900.

KA
4/15/2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100